MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER
COMMANDERS OF THE UNIFIED COMBATANT COMMANDS

SUBJECT: Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 6-8510 - – Department of Defense Information Assurance

The attached Department of Defense Information Assurance (IA) guidance and policy is effective immediately. Secure, interoperable information capabilities that meet both warfighting and business needs throughout the Department's Global Information Grid (GIG) are fundamental to realizing the Joint Vision 2010 goal of Information Superiority. The attached guidance and policy provides the framework for achieving IA by ensuring the availability of systems, the integrity and confidentiality of information, and the authentication and non-repudiation of electronic transactions. These IA services must be employed for all information and systems, both classified and unclassified, and whether information is deemed mission critical, mission support or administrative.

It is recognized that some of the measures called for in the attached guidance and policy cannot be fully implemented immediately; however, the cyber threats and

vulnerabilities to DoD Information Technology (IT) are such that implementation should begin immediately where possible. Subsequent guidance will establish final dates for the completion of specific measures. These dates will take into account the urgency and priority of the IA need and the projected availability of adequate IA solutions.

A DoD Directive covering the attached policy and DoD Instructions on the implementation of the policy will be issued after the normal coordination process.

If you have any questions, please direct them to Mr. Donald L. Jones in the Office of the Director for Infrastructure and Information Assurance. He can be reached at (703) 614-6640 or e-mail donald.l.jones@osd.pentagon.mil.

John Hamre

Attachment: Guidance and Policy for Department of Defense Information Assurance .

Guidance and Policy for Department of Defense Information Assurance

ASD (C3I)

1. PURPOSE: This guidance and policy establishes Department of Defense (DoD) information assurance (IA) policy, assigns responsibilities, and provides technical implementation guidance to enable the secure exchange and use of information necessary to the execution of the DoD mission. This issuance specifically:

1.1. Establishes information system mission categories, defines levels of robustness and specifies requirements for their use, and defines and directs implementation of a defense-in-depth strategy for applying integrated, layered protection of the DoD's information systems and networks.

1.2. In the event of conflict, this guidance and policy takes precedence over DoD Directive 5200.28, DoD Manual 5200.28-M, and DoD Directive C-5200.5 (references (a), (b), and (c)).

2. APPLICABILITY AND SCOPE:

2.1. This guidance and policy applies to:

2.1.1. The Office of the Secretary of Defense (OSD); the Military Departments; the Chairman of the Joint Chiefs of Staff; the Combatant Commands; the Inspector General of the Department of Defense (IG,DoD); the Defense Agencies and DoD field activities (hereafter referred to collectively as "the DoD Components").

2.1.2. All information technologies that are used to enter, process, store, display or transmit DoD information, regardless of classification or sensitivity.

2.2. This policy memorandum does not address additional measures that may be required for the protection of foreign intelligence or counterintelligence information, Sensitive Compartmented Information (SCI) (reference (d)), Single Integrated Operating Plan – Extremely Sensitive Information (SIOP-ESI) (reference (e)), or Special Access Program (SAP) information (reference (f)) that transit DoD information networks.

2.3. This policy memorandum excludes Intelligence Community (IC) information and information systems operated within the DoD which fall under the authority of the Director of Central Intelligence (DCI) as provided for, but not limited to, reference (d). The protection of IC information and information systems not covered in reference (d) shall be coordinated through a process jointly determined between the DoD Chief Information Officer (CIO) and the IC CIO.

3. DEFINITIONS

Terms used in this policy are defined in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009 (reference (g)) or at Enclosure 2.

4. POLICY: It is DoD policy that:

4.1. The DoD shall follow an enterprise-wide IA architecture that implements a defense-in-depth strategy which incorporates both technical and non-technical means and employs multiple protections at different layers within information systems and their supporting communications networks to establish and maintain an overall acceptable IA posture across the DoD. Safeguards shall be applied such that information and information systems maintain the appropriate level of confidentiality, integrity, availability, authentication, and non-repudiation based on mission criticality, classification or sensitivity of information handled (i.e., entered, processed, stored, displayed, or transmitted) by the system, and need-to-know, while maintaining required levels of interoperability. Enclosure 3, Implementation Guidance, provides details on the selection and implementation of safeguards.

4.2. All DoD information systems shall be assigned to a mission category (mission critical, mission support or administrative) that reflects the type of information handled by the system relative to requirements for integrity (including authentication and non-repudiation) and availability services. Mission categories will be determined by the DoD functional domain owner (e.g., command and control, logistics, transportation, medical, intelligence, personnel, financial, etc.) or the responsible DoD Component head in consultation with the information owner. The mission category of systems that handle information from multiple domains shall default to the highest category supported. System mission categories, functional domain, and information owner are defined in Enclosure 2, Definitions.

4.3. All DoD information systems shall employ protection mechanisms that satisfy requirements for high, medium, or basic levels of robustness. Generally, high robustness security services and mechanisms provide the most stringent protection and rigorous security countermeasures, while medium robustness provides for additional safeguards above the DoD minimum and basic robustness is equivalent to good commercial practice. Paragraph E3.5 of Enclosure 3 provides an in-depth discussion of levels of robustness and detailed guidance on their application to IA solutions.

4.4. The DoD defense-in-depth strategy shall be implemented using technical solutions to the maximum extent possible in order to:

4.4.1. Ensure network and infrastructure services provide appropriate confidentiality (e.g., link encryption) and defenses against denial of service attacks (e.g., diversity, routing table protection, planned degraded operation).

4.4.2. Defend the perimeters of well-defined information enclaves (e.g., firewalls, intrusion detection, uniform policy on protocols allowed across perimeter boundaries).

4.4.3. Provide appropriate layers and degrees of protection to all computing environments (e.g., internal hosts and applications).

4.4.4. Make appropriate use of supporting IA infrastructures (e.g., key management, public key certificates, directories).

4.5. Resources sufficient to ensure compliance with this policy memorandum shall be planned, budgeted, allocated and executed.

4.6. Information assurance shall be managed to ensure that the principles contained in this policy memorandum are included in the decision-making processes throughout the entire life cycle of all systems in accordance with DoD Regulation 5000.2R (reference (h)).

4.7. All inter-connections of DoD information systems, both internal and external, shall be managed to continuously minimize community risk. Specifically:

4.7.1. Interconnection of DoD systems at the same classification level shall be in accordance with established connection approval processes and shall be managed so that mutual risk is minimized and the protection of one system is not undermined by vulnerabilities of other interconnected systems.

4.7.2. Interconnections of DoD systems operating at different classification levels shall be accomplished by processes consistent with the philosophy of the Secret and Below Interoperability (SABI) process (reference (i)) that have been approved by the DoD (CIO) and, where appropriate, formally coordinated with the IC CIO.

4.7.3. All connections to non-DoD information systems, including foreign nation systems, shall be accomplished in accordance with established DoD connection approval processes and be coordinated with the IC CIO, as appropriate.

4.7.4. Interconnections of Intelligence Community systems and DoD systems shall be accomplished using a process jointly concurred in by the DoD CIO and the IC CIO.

4.8 DoD information systems processing classified information and national security systems as delineated by Title 10, United States Code, Section 2315 (reference (j)), shall employ mechanisms that satisfy the requirements for high robustness. Such systems shall employ only National Security Agency (NSA) certified COMSEC (cryptographic) products when the information transits public networks or the system or

network handling the information is accessible by individuals who are not cleared for the classified information on the system.

4.9. DoD Components shall acquire COMSEC products and services to protect classified systems through NSA as the centralized COMSEC acquisition authority, or through NSA designated agents.

4.10. DoD information systems processing sensitive information subject to Public Law 100-235 as codified in Title 15, United States Code, Section 278g-3 (reference (k)) shall employ mechanisms that satisfy the requirement for basic robustness. Such systems shall employ products containing either NSA certified or National Institute of Standards and Technology (NIST) validated cryptographic products when the information transits public networks or the system or network handling the information is accessible by individuals who are not authorized to access the information on the system.

4. 11. All security related commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) hardware, firmware, and software components (excluding cryptographic products) required to protect unclassified DoD information systems shall be evaluated and validated prior to acquisition, using criteria and processes established by NSA. All security related components used to protect classified information must be validated by NSA.

4.12. All DoD information systems shall be certified and accredited in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Instruction 5200.40 (reference (l)).

4.13. Access to DoD information systems shall be granted on a need-to-know basis and will be in accordance with DoD Regulation 5200.2R (reference (m)).

4.14. DoD information systems that allow open, uncontrolled access to information made available by the Department, such as information intended for dissemination to the general public (e.g. publicly accessible web servers), or systems that allow unregulated access to and from the Internet shall be isolated from other DoD systems. The isolation may be physical, or may be implemented by technical means such as an approved boundary protection product in accordance with the DoD policy for web site administration (reference (n)).

4.15. Interoperability between DoD and its vendors and contractors will be accomplished using External Certificate Authorities (ECAs) that will operate under a DoD CIO approved process which delivers a level of assurance that meets business and legal requirements as determined by the DoD Comptroller and the DoD General Counsel.

4.16. All DoD information systems shall be monitored in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the security of DoD operations or information technology resources. The information systems are also subject to active penetrations and other forms of testing used to complement

monitoring activities in accordance with DoD Directive 4640.6 (reference (o)), and applicable laws and regulations.

4.17. Use of public key certificates in DoD information systems shall be in accordance with the DoD public key infrastructure policy (reference (p)).

4.18. All DoD personnel and support contractors shall be trained and appropriately certified to perform the tasks associated with their designated responsibilities for safeguarding and operating DoD information systems in accordance with joint USD (P&R) and ASD (C3I) guidance (reference (q)).

4.19. Public domain software products (i.e., freeware) shall not be used in DoD information systems unless an official requirement is established, the product is assessed for information assurance impacts, and approved for use by the responsible Designated Approving Authority (DAA).

5. RESPONSIBILITIES:

5.1. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)), in his capacity as the DoD Chief Information Officer (CIO), shall:

5.1.1. Monitor and provide oversight for all DoD IA activities.

5.1.2. Develop and promulgate additional DoD IA guidance consistent with this memorandum.

5.1.3. Ensure that all DoD information systems are assigned to a mission category not later than one year from the date of this document.

5.1.4. Ensure the integration of IA initiatives with critical infrastructure protection (reference (r)) sector liaisons.

5.1.5. Establish a formal coordination process with the IC CIO to ensure proper protection of IC information within the DoD.

5.1.6. Manage the Defense-wide Information Assurance Program (DIAP), that shall:

5.1.6.1. Provide for the planning, coordination, integration, and oversight of all DoD IA activities.

5.1.6.2. Establish and monitor IA readiness as an integral part of the DoD mission readiness criteria.

5.1.6.3. Maintain liaison with the office of the IC CIO to ensure continuous coordination of DoD and IC IA activities and programs.

5.2. The Heads of DoD Components shall:

5.2.1. Ensure compliance with this policy memorandum.

5.2.2. Develop and implement an IA program consistent with the enterprise-wide IA architecture and the DoD defense-in-depth strategy focusing on protection of Component-specific information and systems (i.e., sustaining base, tactical, C4I interfaces to weapon systems.) and ensure that:

5.2.2.1 All information systems implement access control and intrusion detection at system perimeter boundaries and within the system/network management components.

5.2.2.2. Classified or sensitive information handled by systems that are accessible by unauthorized (lesser cleared) individuals is protected by access control and encryption in addition to other, non-technical, security measures.

5.2.2.3. All electronic transactions are provided data integrity and authentication by the appropriate combination of digital signature, keyed hash, and encryption mechanisms.

5.2.3. Plan, budget and execute adequate resources in support of IA.

5.2.4. Ensure that Designated Approving Authorities (DAAs) accredit each information system under their jurisdiction in accordance with the DITSCAP, (reference (l)).

5.2.5. Develop Memorandums of Agreement (MOA), as appropriate, for interconnection of information systems managed by multiple DAAs.

5.2.6. Assign mission categories to Component-specific systems not later than one year from the date of this policy.

5.2.7. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all system technologies and supporting infrastructures including sustaining base, tactical, and C4I interfaces to weapon systems.

5.2.8. Ensure that IA awareness, training, education, and professionalization are provided to all personnel commensurate with their respective responsibilities for using, operating, administering, and maintaining DoD information systems in accordance with reference (q).

5.2.9. Comply with established connection approval processes for all information systems connections.

5.2.10. Share techniques, technologies, and R&D relating to IA with other DoD components.

5.2.11. Provide for an IA monitoring and testing capability in accordance with reference (o) and applicable laws and regulations.

5.2.12. Provide for a vulnerability and incident response and reporting capability.

5.2.13. Take appropriate actions in response to system vulnerability alert notifications issued through the Information Assurance Vulnerability Alert (IAVA) Process (reference (s)).

5.2.14. Report all systems security incidents in accordance with CJCS instructions.

5.2.15. Take action in response to Information Operation Conditions (INFOCONs) as directed by the CJCS. (reference (t)).

5.2.16. Comply with DoD COMSEC instructions and regulations.

5.2.17. Ensure that contractors and agents comply with requirements to protect classified and sensitive unclassified information.

5.2.18 Ensure that all COTS products acquired for security functions have been evaluated under criteria established by NSA.

5.2.19. Secure information systems and networks by acquiring and employing IA solutions in accordance with the robustness policies described in the implementation guidance at enclosure 3, Implementation Guidance.

5.2.20. Consult the IA Technical Framework (IATF) and published Common Criteria (CC) Protection Profiles for guidance regarding common classes of network and system attacks, interoperability and compatibility with the defense-in-depth strategy, and IA solutions that should be considered to counter attacks.

5.2.21. Acquire IA solutions that have been evaluated using the Common Criteria Evaluation and Validation Scheme based on the National Information Assurance Program (NIAP) process.

5.2.22. Implement IA solutions following the risk assessment process outlined in the DITSCAP, (reference (l)) to insure proper IA risk management and sustainment.

5.2.23. Ensure that access to DoD information systems and access to specified types of information (e.g., intelligence, proprietary) under their jurisdiction is granted only on a need to know basis.

5.3. The Chairman, Joint Chiefs of Staff, in addition to the responsibilities specified in paragraph 5.2., shall:

5.3.1. Ensure that Combatant Commanders incorporate appropriate IA elements in the generation of requirements for systems support to Joint and Combined operations.

5.3.2. Validate requirements for foreign nation access to DoD-wide elements of the information infrastructure (e.g., the Defense Information Systems Network (DISN)). Validated requirements shall be submitted to the appropriate connection approval process.

5.3.3. Manage the DoD Information Operations Condition (INFOCON) process and declare changes in the DoD INFOCON, as appropriate.

5.4. The Commander, JTF-CND shall:

5.4.1. Coordinate and direct DoD-wide computer network defense operations to include:

5.4.1.1. Actions necessary for a synchronized defense of DoD computer systems and networks (e.g., network patches, firewall rules).

5.4.1.2. Actions necessary to stop a computer network attack (CNA), limit damage from a CNA, and restore effective computer network service following a CNA.

5.4.2. Issue INFOCONs to alert DoD Components of DoD-wide cyber situations that threaten the DoD and require increased awareness and specific defensive postures.

5.5. The Director, National Security Agency (NSA), in addition to responsibilities specified in paragraph 5.2., shall:

5.5.1. Implement an IA intelligence capability responsive to requirements for the DoD, less DIA responsibilities.

5.5.2. Provide IA services to DoD Components as required to assess the threat to, and vulnerability of, IA technologies.

5.5.3. Serve as the DoD focal point for INFOSEC R&D in support of IA requirements to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.5.4. Lead the development of an IA technical framework in support of the defense-in-depth strategy and provide engineering support and other technical assistance for its implementation within DoD.

5.5.5. Establish and manage a program for the evaluation and validation testing of commercially developed IA products in categories directed by the DoD CIO.

5.5.6. Certify cryptographic products that are used to protect classified information or information processed by national security systems as delineated by Title 10, United States Code, Section 2315 (reference (j).

5.5.7. Certify cryptographic modules required for protection of sensitive information delineated in Title 15, United States Code, Section 278g-3 (reference (k)).

5.5.8. Establish criteria and processes for evaluating and validating all security related commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) hardware, firmware, and software components (excluding cryptographic modules) required to protect unclassified DoD information systems. Validate all security-related components used to protect classified information.

5.5.9. Coordinate activities of the National Security Incident Response Center (NSIRC) (reference (u)) with other DoD Components to integrate NSIRC efforts into protection of the enterprise.

5.5.10. Act as the centralized COMSEC acquisition authority.

5.6. The Director, Defense Intelligence Agency (DIA), in addition to the responsibilities specified in paragraph 5.2., shall:

5.6.1. Provide finished intelligence on IA to DoD Components.

5.6.2. Develop, implement, and oversee an IA program for layered protection of the DoD Intelligence Information System (DoDIIS).

5.6.3 Manage the connection approval process for Joint Worldwide Intelligence Communications System (JWICS) elements of the DISN in accordance with the process determined under paragraph 4.7.4., above.

5.7. The Director, Defense Information Systems Agency (DISA), in addition to the responsibilities specified in paragraph 5.2., shall:

5.7.1. In coordination with NSA, develop, implement and oversee a single IA strategy for layered protection (defense-in-depth) of the DoD-wide elements of the information infrastructure.

5.7.2. Manage connection approval processes for Secret Internet Protocol Router Network (SIPRNET) and Unclassified But Sensitive Internet Protocol Network (NIPRNET) elements of the DISN.

5.7.3. Operate and maintain, in coordination with the other DoD Components, an information system monitoring and incident response center.

5.7.4. Coordinate with and support the JTF-CND.

5.7.5. In coordination with the Joint Staff, NSA, and DIA as required, maintain security accreditation of the DoD-wide elements of the information infrastructure.

5.7.6. Coordinate the DoD Information Assurance Vulnerability Alert (IAVA) Process (reference (s)).

5.7.7. Implement and maintain the DITSCAP, (reference (l)), for security certification and accreditation of DoD component and contractor information technology systems.

5.8. The Director, Defense Security Service (DSS), in addition to the responsibilities specified in paragraph 5.2. shall:

5.8.1. Monitor information system security practices of DoD contractors processing classified information in accordance with DoD Directive 5220.22M (reference (v)).

5.8.2. Inspect COMSEC accounts as a part of regular industrial security inspections at DoD contractor facilities.

5.9. Each Designated Approving Authority (DAA) shall:

5.9.1. Be responsible for the security of all systems under his or her jurisdiction.

5.9.2. Review and approve security safeguards and issue accreditation statements for each system under their jurisdiction, based on the acceptability of the safeguards and compliance with the DITSCAP (reference (l)).

5.9.3. Ensure that all required safeguards, as specified in accreditation documentation, are implemented and maintained.

5.9.4. Identify security deficiencies and initiate appropriate action to achieve an acceptable security level as required.

5.9.5. Ensure that Information Systems Security Managers (ISSMs), Information Systems Security Officers (ISSOs), and Systems Administrators (SAs) are designated for all systems under their jurisdiction, and that they receive the level of training necessary and appropriate certification to perform the tasks associated with their assigned responsibilities.

5.9.6. Verify that data ownership is established for each system under their jurisdiction and that the system has been assigned to a mission category.

5.9.7. Ensure that, when required, systems provide mechanisms for controlling access to specific information (e.g., intelligence, proprietary) based on mission and need-to-know determinations made by information owners.

5.9.8. Ensure that a process for reporting security incidents is established.

5.10 Each Information Systems Security Manager (ISSM) shall:

5.10.1. Serve as the focal point for policy and guidance on IA matters within their activity.

5.10.2. Provide policy and program guidance to subordinate activities.

5.11. Each Information Systems Security Officer (ISSO) shall:

5.11.1. Ensure that systems for which they have cognizance are operated, used, maintained, and disposed of in accordance with the system accreditation package security policies and practices.

5.11.2. Have the authority to enforce IA policies and safeguards on all personnel having access to the system for which the ISSO has cognizance.

5.11.3. Ensure that users have the required security clearances, authorization and need-to-know, have been indoctrinated, and are familiar with required security practices prior to being granted access to the system.

5.11.4. Ensure that audit trails are reviewed periodically.

5.11.5. Report all security incidents as directed by the DAA.

5.11.6. Report on the IA posture of the information system, as required by the DAA.

5.12. Each System Administrator (SA) shall:

5.12.1. Work closely with the ISSO to ensure the system is used properly.

5.12.2. Assist the ISSO in maintaining system configuration controls and need-to-know information protection mechanisms.

5.12.3. Advise the ISSO of security anomalies or integrity deficiencies.

5.12.4. Administer, when applicable, user identification or authentication mechanism(s) of the system.

5.12.5. Perform system backups, software upgrades and system recovery, including the secure storage and distribution of backups and upgrades.

6. EFFECTIVE DATE: This policy is effective immediately.

Enclosures – 3
1. References
2. Definitions
3. Implementation Guidance

(Encl. 1)

–E1 ENCLOSURE 1
REFERENCES

(a) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

(b) DoD 5200.28-M, "ADP Security Manual," January 1973 and Change 1, June 24, 1979

(c) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 21, 1990

(d) DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 13, 1999

(e) SM-313-83, "Safeguarding the Single Integrated Operational Plan (U)," May 10, 1983

(f) DoD Directive O-5205.7 "Special Access Program (SAP) Policy," January 13,1997.

(g) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009 rev 1, "National Information Systems Security Glossary," January 1999

(h) DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," March 23, 1998

(i) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, 'Secret and Below Interoperability (SABI)," March 20, 1997

(j) Title 10, United States Code, Section 2315

(k) Title 15, United States Code, Section 278g-3

(l) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process," December 30, 1997

(m) DoD Regulation 5200.2R, "Personnel Security Program," May 6, 1992

(n) Deputy Secretary of Defense Policy Memorandum, "Web Site Administration," December 7, 1998

(o) DoD Directive 4640.6, "Communications Security (COMSEC) Monitoring and Recording," June 26, 1981

(p) Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," May 6, 1999

(q) Under Secretary of Defense (Personnel and Readiness) and Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Joint Memorandum, "Information Assurance (IA) Training and Certification," June 29, 1998

(r) Presidential Decision Directive/NSC –63, Subject: "Critical Infrastructure Protection," May 22, 1998

(s) Secretary of Defense (SECDEF) Message, The Information Assurance Vulnerability Alert (IAVA) Process, ASD (C3I)_DTG 252016Z June 1998

(t) Chairman of the Joint Chiefs of Staff Memorandum CM-510-99, "Information Operations Condition (INFOCON)", 10 March 1999

(u) National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 503, "Incident Response and Vulnerability Reporting for National Security Systems," August 30, 1993

(v) DoD Directive 5220.22M, "National Industrial Security Program Operating Manual," January 1995 and supplement, February 1995

(Encl. 2)

–E2. ENCLOSURE 2

DEFINITIONS

E2.1. Common Operating Environment. The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), methodology, runtime environment definitions, reference implementations, and methodology, that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product. (DII COE I&RTS)

E2.2. Community Risk. A combination of: 1) the likelihood that a threat will occur within an interacting population; 2) the likelihood that a threat occurrence will result in an adverse impact to some or all members of that populace; and 3) the severity of the resulting impact. (SABI Terms of Reference (TOR))

E2.3. Connection Approval. Authorization to link or join a system with an existing network. (SABI TOR)

E2.4. Criticality. A measure of how important the correct and uninterrupted functioning of the system is to national security, human life, safety, or the mission of the using organization; the degree to which the system performs critical processing. (SABI Handbook)

E2.5. Defense In Depth. The security approach whereby layers of IA solutions are used to establish an adequate IA posture. Implementation of this strategy also recognizes that, due to the highly interactive nature of the various systems and networks, IA solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured..

E2.6. Defense Information Systems Network (DISN). A sub-element of the Defense Information Infrastructure (DII), the DISN is the DoD's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. (DoDI 5200.40, DITSCAP, modified)

E2.7. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security. (DoDI 5200.40)

E2.8. Enclave. An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN) or be based on physical location and proximity.

E2.9. External Certificate Authority. An agent that is trusted and authorized to issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities. Operating requirements for ECAs must be approved by the DoD CIO, in coordination with the DoD Comptroller and the DoD General Counsel. (DoD PKI Policy)

E2.10. Functional Domain. An identifiable DoD functional mission area. For purposes of this policy memorandum, the functional domains are: command and control, space, logistics, transportation, health affairs, personnel, financial services, public works, research and development, and intelligence, surveillance, and reconnaissance (ISR) .

E2.11. Incident and Detection Response Capabilities. The establishment of mechanisms and procedures to monitor information systems and networks; detect, report and document attempted or realized penetrations of those systems and networks; and institute appropriate countermeasures or corrective actions.

E2.12. Information Assurance. Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD S-3600.1)

E2.13. Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying CINC's, Services and agencies (C/S/A) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability. (JTF-CND CONOP)

E2.14. Information Operations Condition (INFOCON). The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack. INFOCON measures focus on computer network-based

protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are: NORMAL (normal activity); ALPHA (increased risk of attack); BRAVO (specific risk of attack); CHARLIE (limited attack); and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions. (CJCS MEMO CM-510-00, 10 March 1999)

E2.15. Information Owner. The organization which creates and is responsible for managing specific information. Usually the principal user of the information created.

E2.16. Information System. The entire infrastructure, organization, personnel and components for the collection, processing, storage, transmission, display, dissemination and disposition of information. (NSTISSI 4009)

E2.17. Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, or society as a whole. (DoDD 5160.54, Critical Asset Assurance Program (CAAP))

E2.18. Intelligence Community Information: Intelligence Community Information refers to Sensitive Compartmented Information and any other information that is classified pursuant to section 1.5(c) of Executive Order 12958 that also bears special intelligence handling markings found in the "Authorized Classification and Control Markings Registry" maintained by the Community Management Staff.

E2.19. Layered Defense. A combination of security services, software and hardware, infrastructures, and processes which are implemented to achieve a required level of protection. These mechanisms are additive in nature with the minimum protection being provided by the network and infrastructure layers.

E2.20. Level of Robustness. The characterization of the strength of a security function, mechanisms, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DoD has three levels of robustness:

a. High: Security services and mechanisms that provide the most stringent available protection and rigorous security countermeasures

b. Medium: Security services and mechanisms that provide for layering of additional safeguards above the DoD minimum.

c. Basic: Security services and mechanisms that equate to good commercial practices.

E2.21. Mission Category. Applicable to information systems, the mission

category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD will has three mission categories:

a. Mission Critical. Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness and must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information).

Sub-Category 1 Mission Critical systems include those defined by the Clinger/Cohen Act as National Security Systems (intelligence activities; cryptologic activities related to national security; command and control of military forces, integral to a weapon or weapons systems; systems critical to direct fulfillment of military or intelligence missions.

Sub-Category 2 Mission Critical systems include those identified by the CINCs which if not functional would preclude the CINC from conducting mission across the full spectrum of operations including: nuclear, readiness (including personnel management critical to readiness), transportation, sustainment, modernization, surveillance / reconnaissance, financial, security, safety, health, information warfare, information security.

Sub-Category 3 Mission Critical systems include those required to perform Department level and Component level core functions.

b. Mission Support. Systems handling information that is important to the support of deployed and contingency forces; must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

c. Administrative. Systems handling information which is necessary for the conduct of day-to- day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information).

E2.22 National Security System. Any telecommunications or information system operated by the Department of Defense, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 10 U.S.C, Section 2315)

E2.23. Network Centric. A holistic view of interconnected information systems and resources that encourages a broader approach to security management than a component-based approach. (SABI TOR)

E2.24. Operating Environment. The total environment in which an information system operates. Includes the physical facility and controls, procedural and administrative controls, personnel controls (e.g., clearance level of the least cleared user).

E2.25. Public Key Infrastructure (PKI). An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for DoD functional domain programs, including generation, production, distribution, control and accounting of public key certificates.

E2.26. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence. (DCID 1/19)

E2.27. Secret and Below Interoperability (SABI) Initiative. An ASD (C3I) directed, JCS sponsored, NSA/DISA executed initiative to enhance Secret and Below Interoperability, measure community risk, and protect the DoD information systems infrastructure. (SABI Handbook)

(Encl. 3)

-E3 ENCLOSURE 3

IMPLEMENTATION GUIDANCE

E3.1. Purpose and Overview

This enclosure provides guidance on the selection of appropriate security countermeasures required to secure the Global Information Grid (GIG) architecture. This document also defines the defense-in-depth (D-i-D) technical strategy underlying the DoD IA concept, in which layers of defense are used to achieve the security objectives. It outlines the D-i-D strategy and points to the Information Assurance Technical Framework (IATF) which provides technical solutions and implementation guidance for specific situations.

E3.1.1. The enclosure is divided into the following sections.

?? Section E3.1. gives the purpose of the document, describes the sections, provides an overview of information assurance, and shows how IA relates to the overall GIG initiative.
?? Section E3.2. describes the operational environment and defines and explains the purpose of mission categories.
?? Section E3.3. addresses defense-in-depth, provides tables that describe high level objectives, discusses target environments for the three major IT focus areas (i.e., networks and infrastructure, enclaves and boundaries, and the computing environment), and the security management infrastructure.
?? Section E3.4. discusses the threat and attack environment and provides a table of common threats and categories of attacks that may target various components of the IT environment (i.e., networks, enclaves, hosts, applications).
?? Section E3.5 discusses levels of robustness for individual security services and mechanisms and how they relate to overall IA solutions.
?? Section E3.6. addresses non-technical countermeasures including: personnel, physical, and procedural security; security training, education and awareness; marking and labeling; incident reporting and response; assessments; and, risk management.

E3.1.2. Information Assurance (IA) services provide security by ensuring the availability of the information system, the integrity and confidentiality of information and the accountability and non-repudiation of parties in electronic transactions. To the degree required, these IA services must be employed for all information and systems in the DoD (i.e., both classified and unclassified, and whether deemed mission critical,

mission support or administrative). Further, the majority of DoD information systems are interconnected such that a security risk assumed by one entity is a risk shared by all those who are a part of the interconnected systems. Security is needed not only for intra-CINC, Service and Agency transactions, but also for transactions among the DoD components, and with other U.S. government departments, allies and trading partners. For these reasons, a comprehensive, common IA strategy becomes very important and all DoD components must cooperate in its development and implementation.

E3.1.3 It is important to keep in mind that there are no "cookbook" solutions to appropriate IA. Any specific implementation is dependent upon an in-depth system security analysis and evaluation which must take into consideration all of the factors (e.g., system mission category, confidentiality requirements, threat, and operating environment) in order to tailor an appropriate defense-in-depth solution for the implementation. Additional detail on security technologies that can satisfy defense-in-depth requirements may be found in the Information Assurance Technical Framework (http://www.iatf.org).

E3.1.4. Figure E3.1-1 below provides an overview of GIG. The diagram shows how IA, computing and network management services, and information distribution services are distributed across the computing and network environment. The diagram lays the groundwork so that the reader may understand the importance of information assurance across all components of the entire GIG architecture.

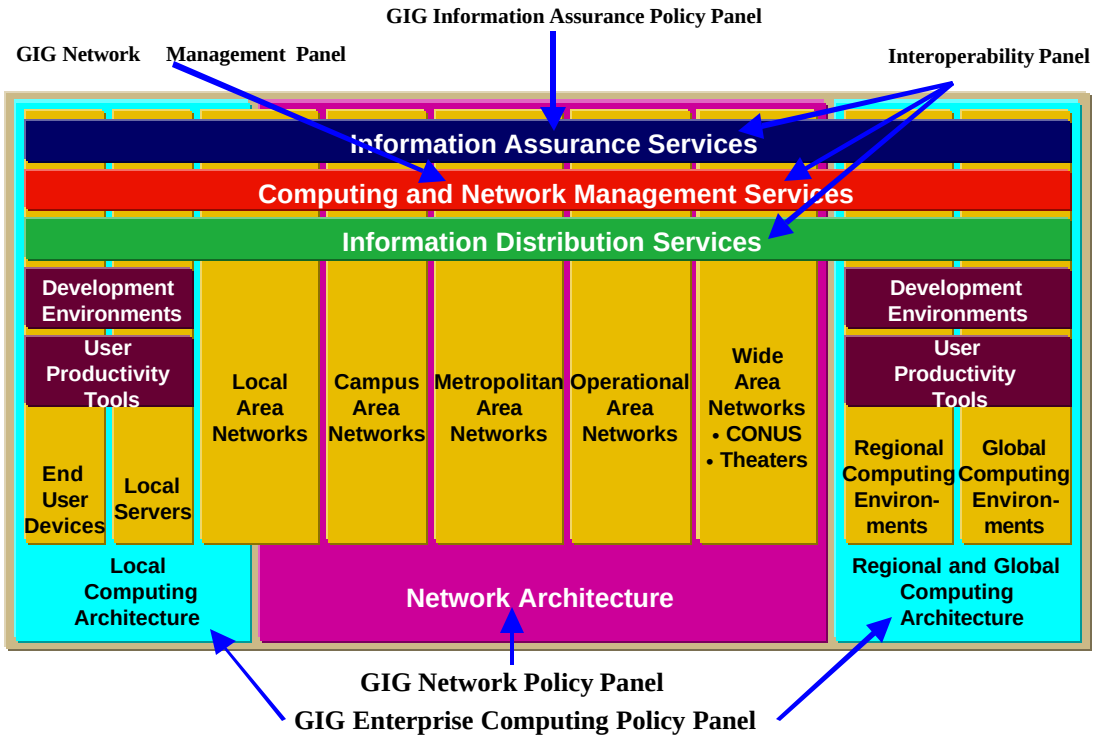

Figure E3.1-1 GIG Computing and Networking Architecture

E3.1.5 The need for securing the DoD information and systems against the full spectrum of cyber threats dictates the use of multiple IA solutions. The fundamental principle is that layers of IA solutions are needed to establish an adequate IA posture. Implementation of this strategy also recognizes that, due to the highly interactive nature of the various systems and networks, any single system cannot be adequately secured unless all interconnected systems are adequately secured. Thus, an IA solution for any system must be considered within the context of the shared risk environment. The D-i-D strategy is predicated on a sound IA technical framework, reflecting technical, performance and best practice standards developed in conjunction with the IT industry. To the greatest extent possible, the recommendations of the IATF must leverage emerging commercial IA technology with available government IA technology. This enclosure describes levels of security robustness in the IA solution components of the defense-in-depth strategy. It is structured in accordance with the defense-in-depth technical layers: the network and infrastructure, the enclave boundary, the computing environment, and overarching security management infrastructure. Figure E3.1-2 below depicts Defense-in-depth from technical, operational, and people related perspectives. The primary focus of this guidance is the technical implementation, however, operational and personnel aspects are discussed in sections E3.6.

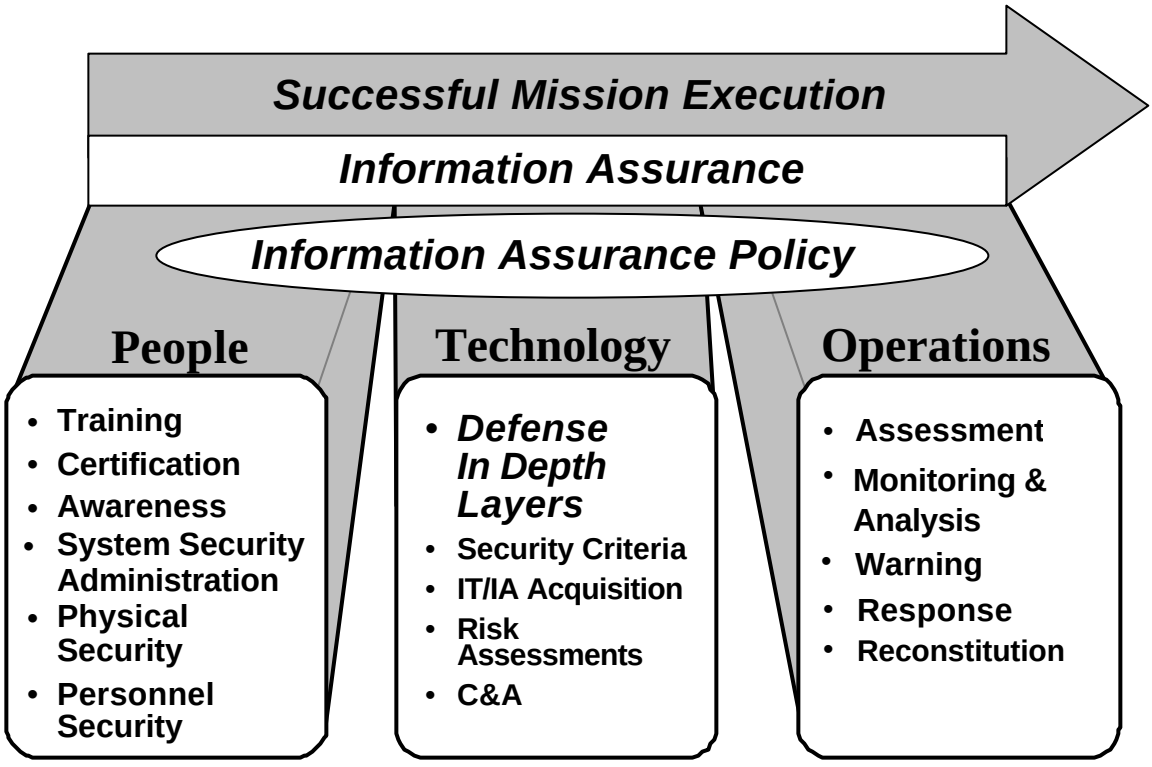

Figure E3.1-2 Defense-in-Depth

E3.1.6 The document tree in Figure E3.1-3 below describes the overall GIG Information Assurance effort and focuses on providing policy and guidance at multiple levels. As the user goes down through the layers of the tree, the technical implementations will more fully describe and support the capability to design security into systems during the development and acquisition processes.

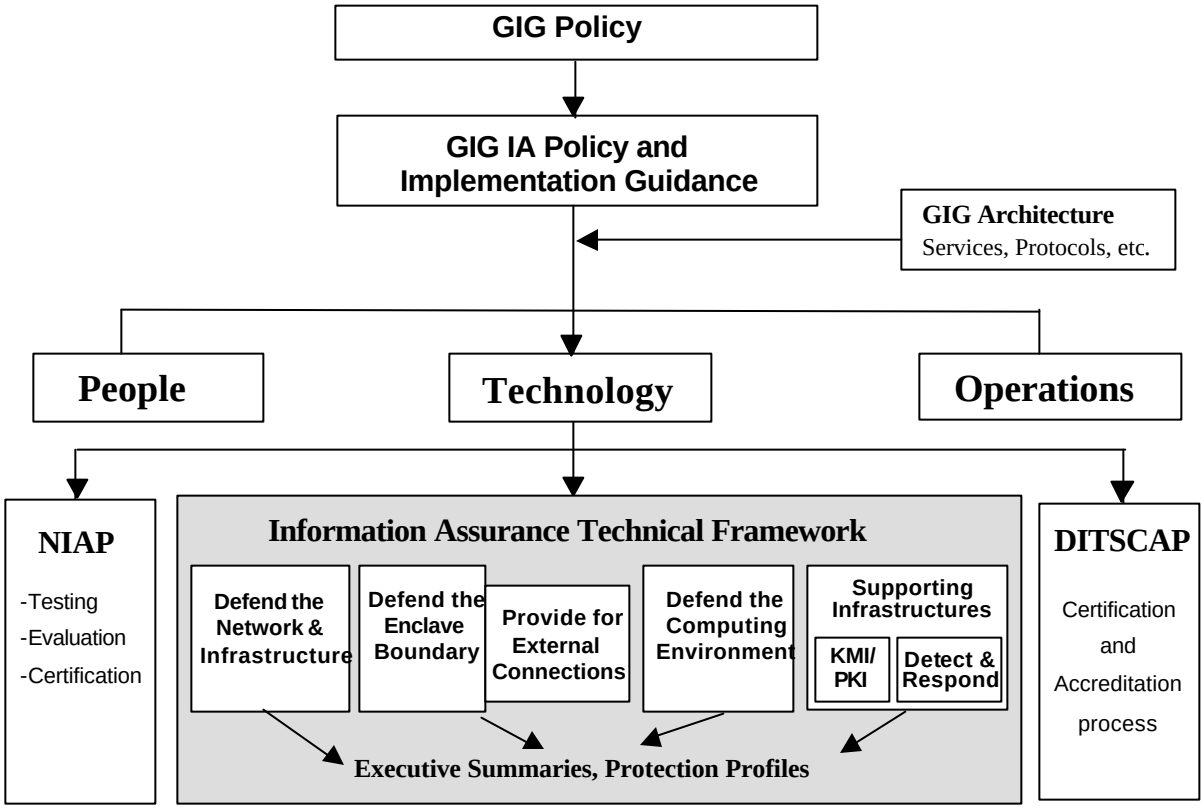

Figure E3.1-3 GIG IA Document Tree

E3.1.7. The terms used in this document are the accepted defense-in-depth terms referenced to the GIG Enterprise Architecture Framework. The GIG framework refers to Uniform Technology Environments or (UTEs). This term is newly defined and has not been translated to the defense-in-depth strategy until this document. A UTE is a common, reusable configuration of technology components. A UTE includes all required elements of hardware and software, including those components for security, management, and distribution services, but excluding applications. Figure E3.1-4 below depicts the use of UTE's within the GIG architecture. However, the GIG Framework does not directly reference the concept of an enclave. The enclave is a very important portion of the D-i-D layering concept and must be addressed in this document. For purposes of this document, an enclave is defined as an environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN) or be based on physical location and proximity. The enclave encompasses both the network layer and the host and applications layer. The enclave is a strategic concept of defense-in-depth since this is the primary layer for firewalls and other perimeter defense mechanisms.

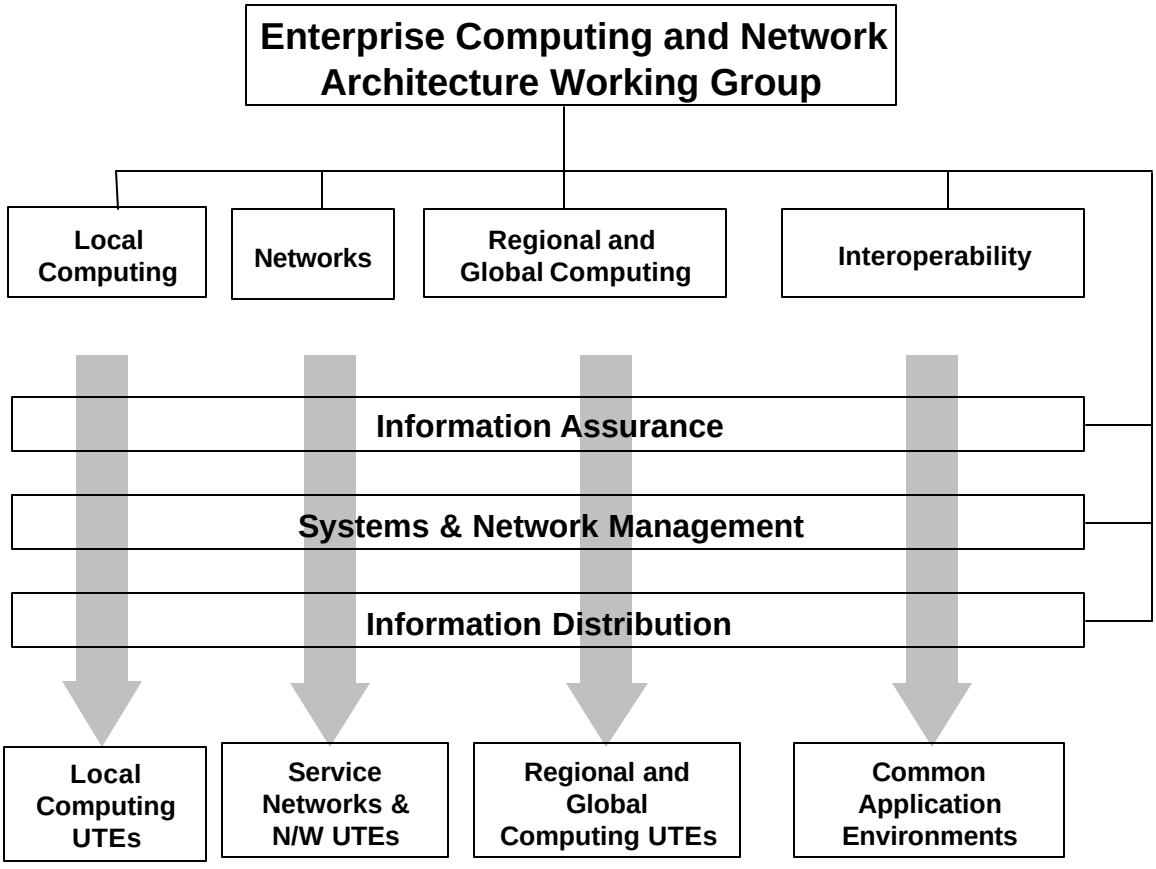

Figure E3.1-4 GIG Enterprise Computing Architecture

E3.2. Operational Environment

E3.2.1. Today, the DoD operates many systems which pass information on commercial network infrastructures between local enclaves. Enclaves typically contain multiple local area networks (LANs) with computing resource components such as clients (users), servers, and local switching/routing, which transmit, process, and store information. The network contains components such as routers and switches which direct the flow of information through the infrastructure. The infrastructure contains the transmission components (satellites, microwave, other RF spectrum, fiber, etc.), most of it commercially leased, to move information across the network. DoD employs the Internet and public switched telephone network backbones, as well as the radio frequency spectrum for voice and data transmission. Figure E3.2-1 represents today's operating environment from a high level networking perspective. Detailed Defense in Depth layers are defined in section E3.3.

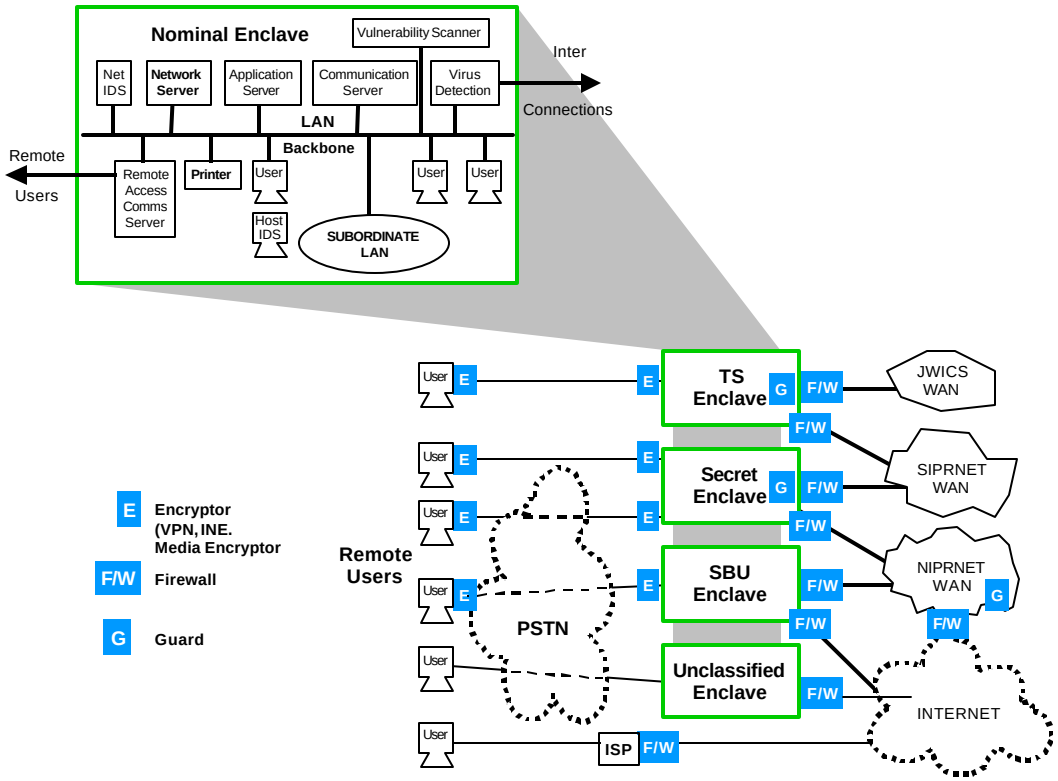

Figure E3.2-1 Operational Environment

E3.2.2. Information transmitted, processed or stored in this environment is currently hierarchically "classified" as Top Secret/ SCI, Top Secret, Secret, Confidential, Sensitive (but Unclassified), or Unclassified. In addition, information can be further tagged with a number of handling caveats.

E3.2.3. While the long standing hierarchical classification scheme is useful for identifying confidentiality needs, it is not very useful in identifying needs for other IA services such as system availability, data integrity, and user authentication. Thus, in addition to classification, information and systems within this environment need to be categorized as Mission Critical, Mission Support or Administrative. Mission categories provide the basis for determining the level of robustness required for availability and integrity services, and are significant from both cost and operational perspectives. They provide a means for prioritizing IT support and allocating resources based on needs for system availability and integrity services. These categories are defined as follows.

E3.2.3.1. Mission Critical: These systems handle information vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified, sensitive, or unclassified information).

E3.2.3.1.1. Sub-Category 1 Mission Critical Systems include those defined by the Clinger/Cohen Act as National Security Systems (intelligence activities; cryptologic activities related to national security; command and control of military forces, integral to a weapon or weapons systems; systems critical to direct fulfillment of military or intelligence missions).

E3.2.3.1.2. Sub-Category 2 Mission Critical Systems include those identified by the CINCs which if not functional would preclude the CINC from conducting their mission across the full spectrum of operations, e.g., nuclear, readiness (including personnel management which is critical to readiness), transportation, sustainment, modernization, surveillance/reconnaissance, financial, security, safety, health, information warfare, and information security.

E3.2.3.1.3. Sub-Category 3 Mission Critical Systems include those required to perform Department-level and Component-level core functions.

E3.2.3.2. Mission Support: These systems handle information important to the support of deployed and contingency forces. Information on these systems must be accurate, but can sustain minimal delays without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

E3.2.3.3. Administrative: These systems handle information which is necessary for the conduct of day-to-day business, but do not materially affect support to deployed or contingency forces in the short term (may be classified but is usually

sensitive or unclassified). It is recognized that this information may be recreated if the need arises.

E3.3. Defense in Depth

The concept of defense–in-depth was presented in the overview section of this document. This section describes the four focus areas of defense-in-depth, discusses target environments and proposes objectives for assurance of each focus area.

E3.3.1 Defend the Network and Infrastructure: The network and infrastructure includes large transport networks and other transmission and switching capabilities including operational area networks (OANs), metropolitan area networks (MANs), campus area networks (CANs), and local area networks (LANs), extending coverage from broad communities to local bases. Figure E3.3-1 depicts a high level view of defend the network and infrastructure layer with suggested placement for information assurance components and mechanisms. Table E3.3-1 lists the high level objectives for the network and infrastructure and should be used to define solutions sets in the architecture framework. The target environment for networks and infrastructure includes data, voice, wireless (e.g. cellular, paging), and tactical networks that support both the operational and strategic DoD missions. These networks can be DoD owned and operated (both service and transport) or leased services (transport layer).

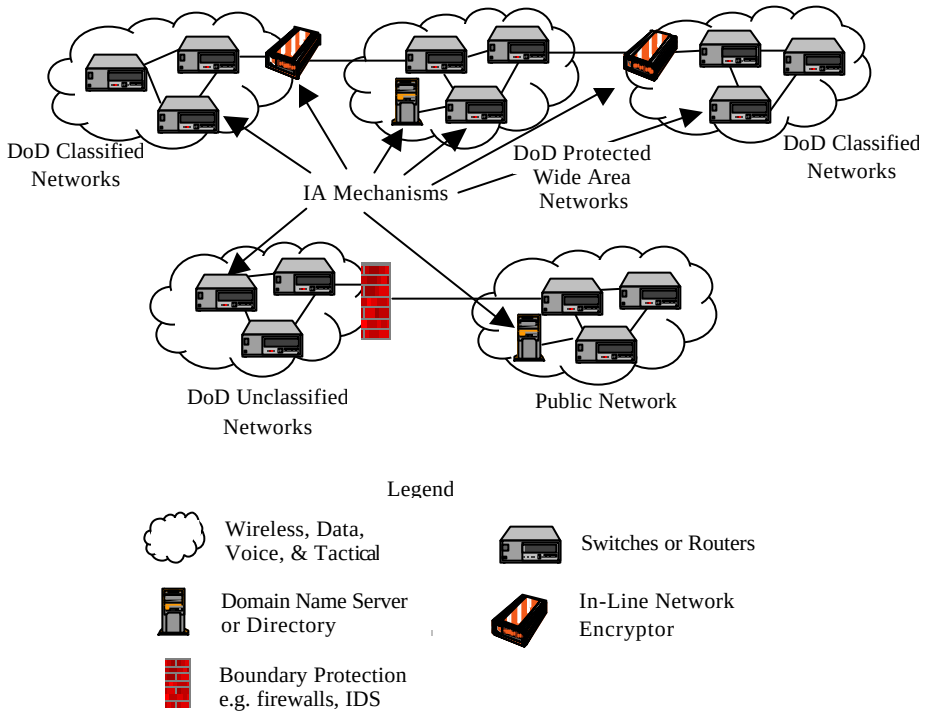

Figure E3.3-1 Defend the Network and Infrastructure

Objectives for Defend the Networks and Infrastructure
?? Ensure that DoD systems and networks follow a consistent architecture
?? Ensure that all data within the DoD Enterprise is adequately protected
?? Ensure that mission critical and mission support networks are protected against denial of service
?? Ensure that networks are visible for monitoring purposes
?? Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event
?? Ensure that the infrastructure does not conflict with other backbone and enterprise networks

Table E3.3-1. Objectives for Networks and Infrastructure

E3.3.2. Defend the Enclave Boundary: Defense of the enclave is focused on the use of IA components to add additional protection at the enclave boundary.. An enclave boundary exists at the point of connection for a LAN or similar network to the service layer.. Figure E3.3-2 depicts a high level view of defend the enclave boundary with suggested placement of IA components and mechanisms (e.g., firewalls and guards). Table E3.3-2 lists the high level objectives for enclave boundary protection and should be used when designing, implementing or integrating an information technology solution that provides enclave boundary protection. Enclave boundary target environments include the following : service layer networks including modem connections; classified LANs within classified WANs (e.g. tunneling information within the SIPRNET); use of virtual private networks on service layers providers; remote enclaves, including remote LANs or systems; laptops that may be connected remotely to different service networks (e.g. Joint Task Force deployments, and high-low transfer and low-to-high transfer.)

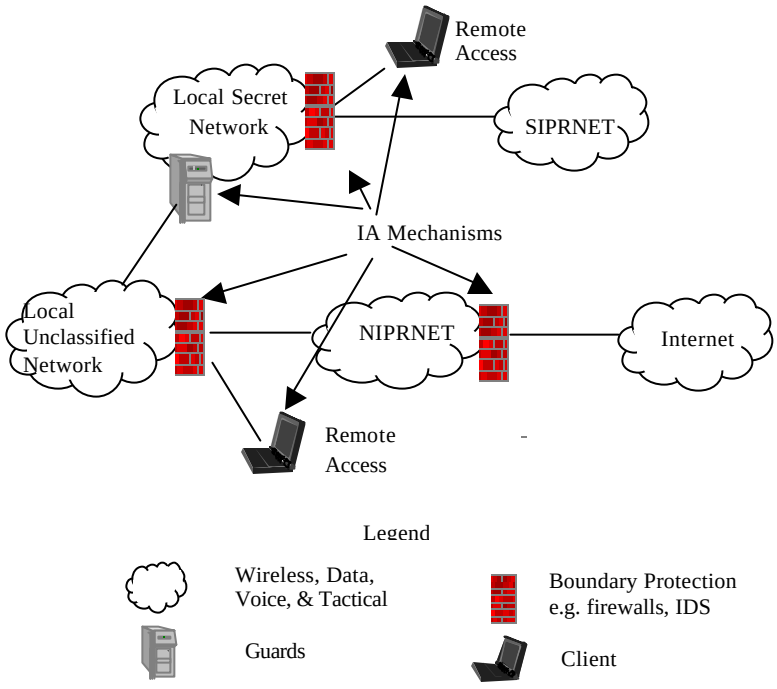

Figure E3.3-2. Defend the Enclave Boundary

Objectives for Defend the Enclave Boundary
?? Ensure that physical and logical enclaves are adequately protected. ?? Enable dynamic throttling of services due to change in risk posture resulting from changing INFOCONs ?? Ensure that systems and networks within protected enclaves maintain acceptable availability and are adequately defended against denial of service intrusions ?? Defend against the unauthorized modification or disclosure of data sent outside enclave boundaries ?? Provide boundary defenses for those systems within the enclave that cannot defend themselves due to technical or configuration problems ?? Provide a risk-managed means of selectively allowing essential information to flow across the enclave boundary ?? Provide protection against systems and data within the protected enclave being undermined by external systems or forces

Table E3.3-2 Objectives for Enclave Boundary Defense

E3.3.3. Defend the Computing Environment: Defense of the computing environment is focused on servers and clients, to include the applications installed on them. An application is any software written to run on a host, and may include portions of the operating system. Figure E3.3-3 depicts a high level view of defend the computing environment. Each computing environment (e.g., user workstation, server, system/subsystem) within the enclave requires a minimum of basic protection. Table E3.3-3 lists high level objectives for computing environment protection. The computing environment includes the end user workstation, both desktop and laptop including peripheral devices; servers including web, application, and file servers; applications such as intrusion detection, e-mail, web, access control and the operating system.

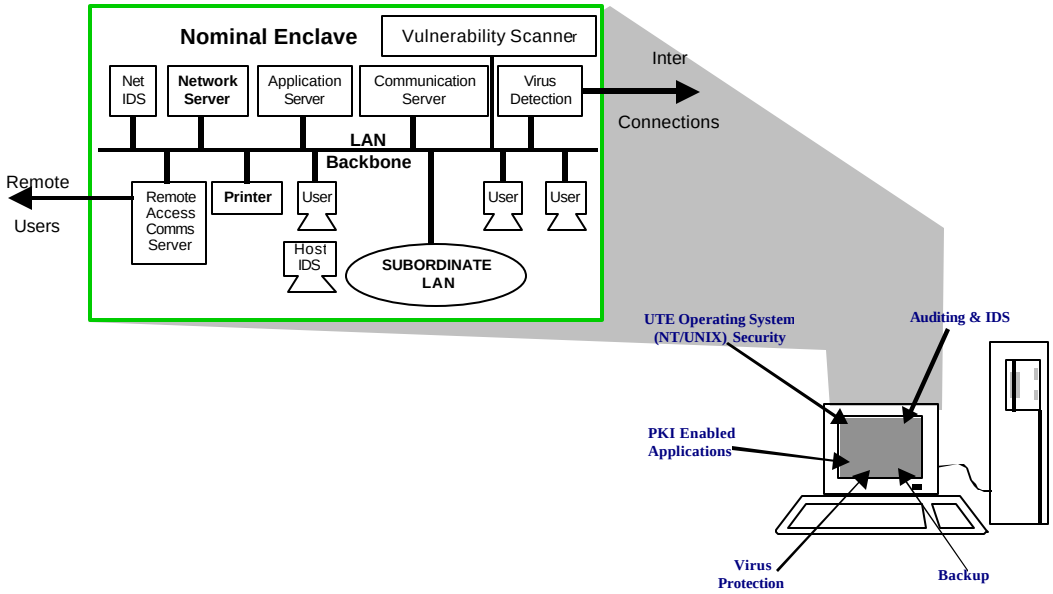

Figure E3.3-3 Defend the Computing Environment

Objectives for the Computing Environment
?? Ensure that hosts and applications are adequately defended against denial of service, unauthorized disclosure, and modification of data
?? Ensure the confidentiality and integrity of data processed by the host or application whether both internal and external to the enclave.
?? Defend against the unauthorized use of a host or application
?? Ensure that a variety of applications can be readily integrated with no reduction in security (e.g., to meet the needs of a Joint Task Force)
?? Ensure adequate defense against the trusted insider
?? Ensure adequate defenses against subversive acts of trusted people and systems, both internal and external

Table E3.3-3. Objectives for the Computing Environment

E3.3.4. Establish Supporting Infrastructures: Supporting infrastructures provide the foundation upon which IA mechanisms are used in the network, enclave, and computing environments for securely managing the system and providing security enabled services. The two primary supporting infrastructures are: (1) key management and (2) detect and respond. Table E3.3-4 lists objectives for supporting infrastructures. Supporting infrastructures provide security services for: networks (e.g. weapons, identify friend or foe, nuclear command and control systems); end-user workstations; servers for web, applications, and files; and, single-use infrastructure machines (e.g. higher level DNS servers, higher-level directory servers). These services apply to both classified and unclassified enclaves.

Objectives for Supporting Infrastructures
??
?? Provide a cryptographic infrastructure that supports key, privilege, and certificate management; and that enables positive identification of individuals utilizing network services
?? Provide an intrusion detection, reporting, and response infrastructure that enables rapid detection and reaction to intrusions and other anomalous events, and that enables operational situation awareness

Table E3.3-4 Objectives for Supporting Infrastructure

E3.3.4.1. Key Management Infrastructure: The key management infrastructure provides a common unified process for the secure creation, distribution, and management of the cryptographic products such as public keys and traditional symmetric keys that enable security services for the network, enclave, and computing environment. Figures E3.3-4 and E3.3-5 depict high level views of the future key management infrastructure architecture and services. KMI-enabled security services such as identification and authentication, access control, integrity, non-repudiation, and confidentiality become increasingly critical as the Department incorporates IA into its electronic systems. Key management provides the common roles and interface processes required to support IA.

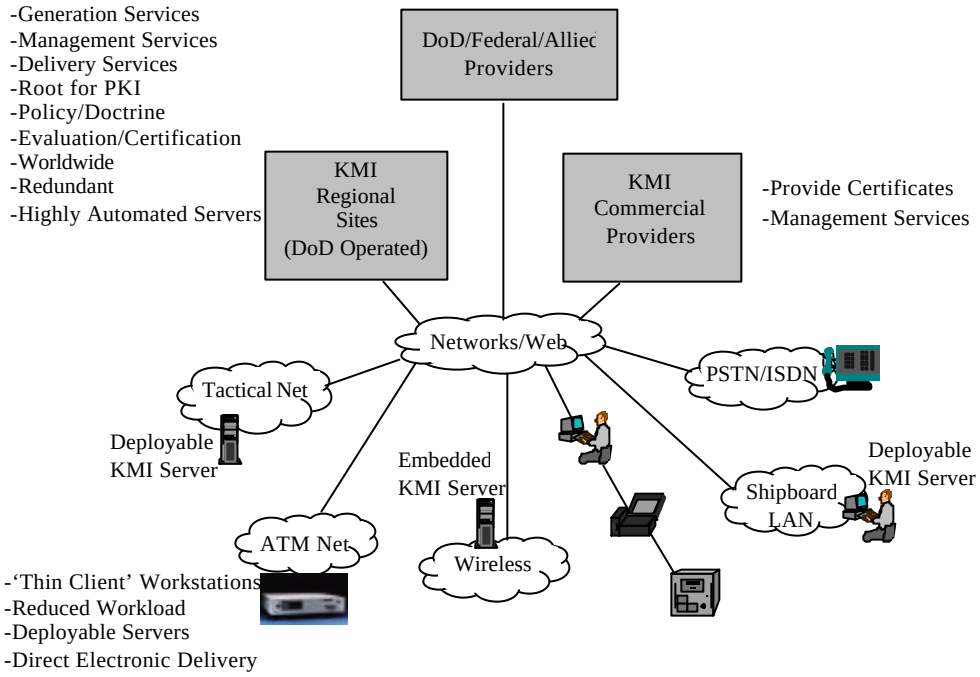

Figure E3.3-4 Key Management Infrastructure

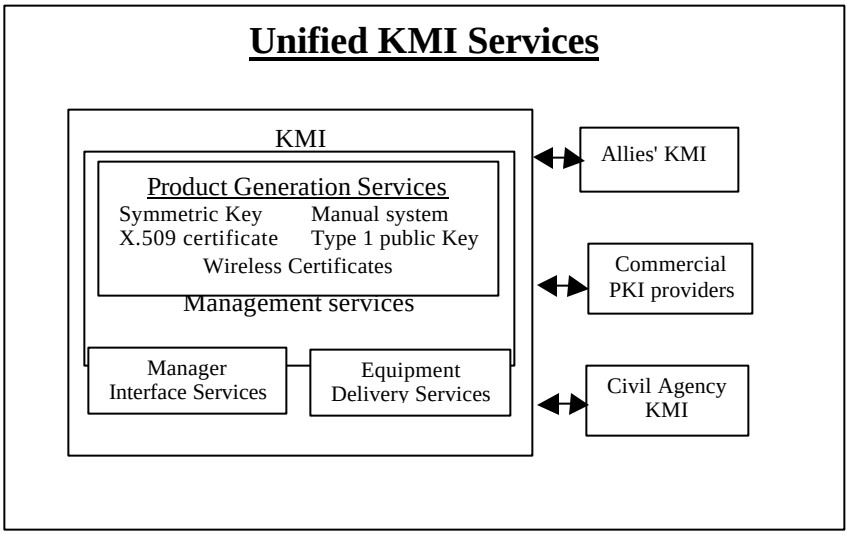

Figure E3.3-5 Key Management Roles and Processes

E3.3.4.2. Detect and Respond: The cyber battlespace is highly fluid, with operational agility critical to effective defense. The detection, reporting, and response infrastructure enables rapid detection of and reaction to intrusions, and enables operational situation awareness and response in support of DoD missions. Local infrastructures support local operation and feed regional and DoD-wide infrastructures, so that DoD can react quickly, regardless of the scale of the intrusion. Figure E3.3-6 depicts a high level view of the Detect and Respond process

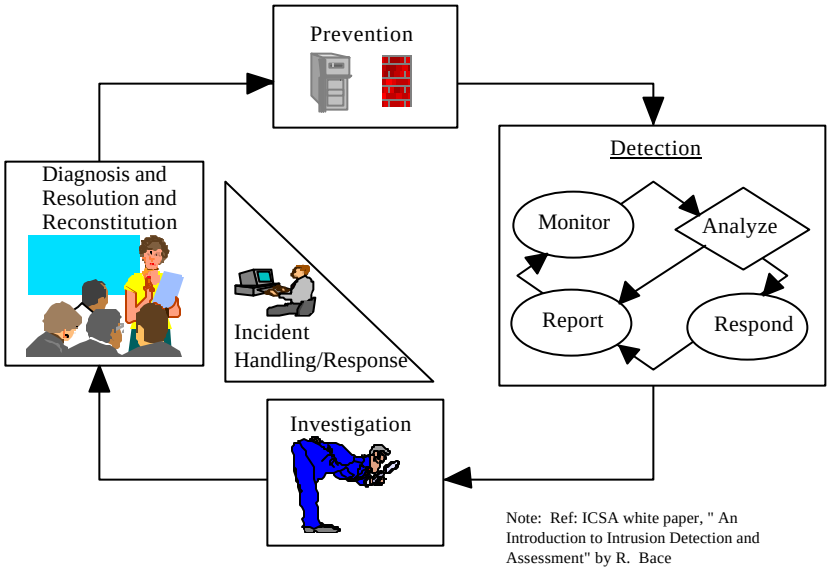

Figure E3.3-6 Detect and Respond Process

E3.4. Threats and Attacks

Threat is defined as any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. Threats may vary based on the motivations and capabilities of adversaries. Threat should be considered from a mission viewpoint as well as from an information processing perspective. Threats must be defined in terms of the threat environment in which the mission will be accomplished. Attack is defined as an attempt to gain unauthorized access to an information system's services, resources, or information or the attempt to compromise an information system's integrity, availability, or confidentiality. Factors to consider when determining the threat to a particular solution include: types of attacks, level of access, risk tolerance, expertise, and resources available to the adversary. Attacks can also be defined in many ways. They can include malicious attacks (e.g., virus, worm, Trojan horse, masquerading), unintentional attacks (e.g., malfunction, human error), and physical attacks (e.g., fire, water, battle damage, power loss). Analysis of potential threats and the countermeasures required to maintain the appropriate confidentiality, integrity, and availability of the information is required to define the best practices to mitigate risk and support defense-in-depth. Table E3.4-1 provides common threat considerations and Table E3.4-2 provides categories of attacks.

All these factors should be considered when designing a system.

Common Threat Considerations

✍ Insider intrusions - both human error and malicious
✍ Network based attacks both systematic and random
  ✍ Jamming of networks both malicious and inadvertent
  ✍ Flooding
  ✍ Theft of service
  ✍ Disruption of network management communications and services
  ✍ Unauthorized access to network operations and management
✍ Unauthorized intrusions by remote operators
✍ Malicious software developers and software
✍ Malicious hardware developers and hardware
✍ Overrun by adversaries
✍ Unauthorized access by others with physical access

Table E3.4-1 Common Threat Considerations

Passive Intercept Attacks – include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing identification numbers and passwords. Passive intercept of network operations can give adversaries indications and warnings of impending actions. **Network-Based Attack**s – include attempts to circumvent or break security features, introduce malicious code or to steal or modify information. These include attacks mounted against a network backbone, exploitation of information in transit, electronic penetrations into an enclave, or attacks on an authorized remote user when she attempts to connect to an enclave. **Close-in Network-Based Attacks** – attempt to execute network-based attacks to penetrate an enclave's protection where the adversary gains access at a point inside the network and infrastructure protection boundary. **Insider Attacks** – are performed by individuals who are authorized physical access to the system or network or have authorized electronic access to that system or network. Malicious insiders have the intent to eavesdrop, steal, or damage information, or to deny access to other authorized users. Non-malicious attacks (typically resulting from carelessness or lack of knowledge) are also considered threats since their actions may have security consequences. **Hardware/Software Distribution Attacks** – focus on the malicious modification of hardware or software at the factory or modification or substitution during distribution.

Table E3.4-2 Categories of Attacks

E3.5 Levels of Robustness

E3.5.1. Robustness describes the strength of mechanism (e.g., the strength of a cryptographic algorithm) and design assurance (i.e. confidence measures taken to ensure proper mechanism implementation) for a technical IA solution. IA solutions in the defense-in-depth strategy will be at one of three defined levels of robustness: High, Medium, or Basic. Designating levels indicates a degree of robustness of the solution. Evaluation Assurance Level (EAL) levels, defined in the International Common Criteria, and classes of certificates, defined in the PKI roadmap, indicate a degree of confidence in the security attributes of the products they relate to. As security mechanisms improve over the years, the robustness of security products should also improve, and more robust products can be incorporated in security solutions. The more robust a particular security attribute is, the greater the level of protection it provides to the security services it supports. Assigning levels of robustness for integrity, availability and confidentiality for all DoD information systems is another means for ensuring the most cost effective and best use of IA solutions, including COTS solutions. When implementing IA solutions, they will be at a designated robustness level except where noted. It is also possible to use non-technical measures to achieve robustness. For example, physical isolation and protection of a network can be used to provide confidentiality. In these cases, the level of technical solution robustness may be reduced or eliminated. The three levels of robustness discussed below are based on the robustness strategy presented in the IATF. It should be noted that today's technology could support development of more stringent protection and rigorous security countermeasures, however, development costs would far exceed acceptable budget limits. Therefore, the term high robustness, used here, is relative to the other levels of robustness, including those of the IATF robustness strategy, and does not indicate the best that could be developed in an unrestrained environment

E3.5.1.1. High robustness security services and mechanisms provide the most stringent protection and rigorous security countermeasures. High robustness includes:

- ?? NSA-certified Type 1 cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash
- ?? Hardware security tokens (e.g., smartcard) that protect the users private key and the crypto-algorithm implementation
- ?? NSA Type 1 cryptographically authenticated access control (e.g., digital signature, public key cryptography based, challenge/response identification and authentication)
- ?? High assurance security design, such as specified by NSA or the International Common Criteria (CC) at a minimum an Evaluated Assurance Level (EAL) greater than 4.
- ?? Class 5 PKI Certificates and/or NSA-certified key management
- ?? Solutions evaluated and certified by NSA.

E3.5.1.2. Medium robustness security services and mechanisms

provide for additional safeguards above the DoD minimum. Medium robustness includes:

- ?? NIST FIPS validated cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash (see algorithm table E3.5-3)
- ?? Hardware security tokens that protect the users private key
- ?? NIST cryptographically authenticated access control (e.g., digital signature, public key cryptography based, challenge/response identification and authentication)
- ?? Good assurance security design such as specified in CC as EAL3 or greater.
- ?? Class 4 PKI Certificates and/or NSA-certified key management
- ?? Solutions evaluated and validated under the Common Criteria Evaluation validation scheme and/or NSA

E3.5.1.3. Basic robustness is equivalent to good commercial practice. Basic robustness includes:

- ?? NIST FIPS validated cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash (see algorithms at Table E3.5-4)
- ?? Software tokens (certificate held in software on the user's workstation)
- ?? Authenticated access control (e.g., digital signature, public key cryptography based, challenge/response identification and authentication or pre-placed keying material)
- ?? CC EAL 1 or greater assurance
- ?? Class 3 PKI Certificates or pre-placed keying material (see reference (p)for the policy on migration to Class 4 Certificates.)
- ?? Solutions evaluated and validated under the Common Criteria Evaluation Validation Scheme and/or NSA

E3.5.2. While paragraph E3.5.1. focuses on the robustness of individual security services and mechanisms, the robustness of a network solution must be considered in the context of defense-in-depth (see section E3.3) and the threat environment in which the system operates. For instance, a system operating on a protected backbone between secure enclaves may not require additional mechanisms for authentication and access control. In addition, if community of interest separation is provided through encryption, it will require less robust solutions.

E3.5.3. The tables below are tools for use in a disciplined system security engineering approach for building or replacing systems. They cover the major defense in depth areas but are not all-inclusive for every system requirement and should not be used as a substitute for good systems security engineering. The robustness indicated is the minimum that should be considered for the defense in depth application in the environment listed. However, more robust solutions should always be considered during the in-depth security analysis of system requirements. In addition, as information assurance technology improves, and systems are replaced or upgraded, higher robustness

solutions should always be considered.

E3.5.3.1. Availability ensures that the resources and data are in place, at the time and in the form needed by the user. Availability can be enhanced by access control, which limits access to authorized users only. Integrity ensures that data has not been altered or destroyed and is achieved through the use of digital signatures or keyed hash schemes. Non-repudiation provides the ability to prove to a third party that an entity did indeed participate in a communication. Non-repudiation is provided by the authenticating characteristics of digital signatures. Minimum robustness requirements for availability, integrity, and non-repudiation are shown in Table E3.5-1.

Security Service	**Robustness**		
	High	**Medium**	**Basic**
Availability		Mission Critical over an unencrypted network.	1. Mission support and Administrative over any network. 2. Mission Critical over an encrypted network.
Integrity, Non-repudiation		1. Mission Critical over an unencrypted network. 2. Network Management commands over an unencrypted network.	1. Mission Critical over an encrypted network. 2. Mission support and Administrative over any network. 3. Network Management commands over an encrypted network.

Table E3.5-1 Security Services Robustness

E3.5.3.2. : Access Control is used to limit access to networked resources (hardware and software) and data (stored and communicated). The main elements of access control are identification and authentication (I&A) and authorization. Passwords, tokens, and certificates are used to achieve authenticated access control. Table E3.5-2 gives examples of minimum robustness requirements for access control mechanisms in particular situations.

Defense in Depth Application examples	Level of Robustness for Access Control	
	Encrypted and/or Physically Isolated Network	**Unencrypted or not Physically isolated Network**
Defend the Network		
Access to DoD Network Management Centers and all Network Management control commands to managed GIG components (e.g. routers, switches), as well as inter-element commands (e.g. router table propagation)	Basic	Medium
Defend the Enclave		
All interconnections between Enclaves or LANs operating at different classification levels, (e.g. TS to Secret, Secret to Unclassified) will only be through a well-defined and controlled gateway. (NOTE: Connection between different classification levels allow lower classified or unclassified data from the higher classified system to be moved to the lower classified or unclassified system (e.g., unclassified data on a secret system to an unclassified system). In addition, unclassified data from an unclassified system can be moved to a classified system with the use of a well-defined and controlled gateway.	Medium + (The level of robustness for this case, which is also know as a high assurance guard, is medium, however additional design assurance is required and must have an EAL greater than 4.)	Medium + (The level of robustness for this case, which is also know as a high assurance guard, is medium, however additional design assurance is required and must have an EAL greater than 4.)
All boundaries between Enclaves at the same sensitivity level and the WAN will be protected	Basic	Basic- for mission support and administrative information Medium- for Mission critical
(NOTE: All gateways at boundaries between Enclaves and WAN will contain an intrusion detection / attack sensing and warning capability. All interconnections between Enclaves or LANs operating at different classification levels should be designed and analyzed to reduce covert channels)		
Defend the Computing Environment		
User Logon to a workstation to gain access to network resources	Basic	Basic
User access to servers (e.g. Web servers, database servers, file servers) or other components storing Special Compartmented, Special Access, or other Mission Critical information, will use authenticated access.	Basic	Medium

User accesses to servers (e.g. Web servers, database servers, file servers) or other components storing mission support or administrative, will use authenticated access.	Basic	Basic
All Network Management control commands to managed GIG components (e.g. routers, switches), as well as inter-element commands (e.g. router table propagation) in the Enclave will emp loy authentication.	Basic	Medium
All Mission Critical, Mission Support and Administrative transactions, to include individual (non-organizational) e-mail and e-commerce, will be secured with a digital signature.	Basic	Basic- for mission support and administrative information Medium- for Mission Critical information

Table E3.5-2 Access Control Robustness Examples

E.3.5.3.3. Encryption is a primary method of ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes. It is used to provide confidentiality, data separation or privacy. Table E3.5-3 provides robustness guidance for data encryption robustness. Note that when information is encrypted for the purposes of data separation or privacy, it is always tunneled through a network that is also encrypted for confidentiality.

Purpose of Encryption	Data classification / Network Type	Minimum Robustness of Algorithm
Confidentiality	TS through Secret	High
	TS through Commercial	High
	Secret through Commercial	High
	Unclassified Sensitive through Commercial	Basic
Data Separation	Secret through TS	Medium
	U through TS	Medium
	U through Secret	Medium
Privacy	TS through TS	Basic
	Secret through Secret	Basic
	Unclassified through Unclassified Sensitive	Basic

Table E3.5-3 Data Encryption Robustness

E3.5.3.4. Cryptographic functions include encryption, hash, signature and key exchange algorithms. These algorithms are used to protect the confidentiality and/or integrity of information. Table E3.5-4 lists currently available algorithms. It includes algorithms that are often encountered in commercial products primarily for reference purposes. The number of bits or the length of the cryptographic key used in the algorithm and the design assurance of the algorithm are directly related to its robustness and will determine whether the NIST certified algorithms listed in Table E3.5-4 are basic

or medium robustness. Within the Department of Defense, only NSA or NIST certified cryptographic algorithms may be used (reference (c)) unless otherwise authorized (reference (n)). See Chapter 4 of the IATF (http://www.iatf.org) for a detailed description of algorithm robustness.

Algorithm	**Commercially Available (Reference)**	**NIST Certified Basic/Medium Robustness**	**NSA Certified High Robustness**
Encryption Algorithm	RC4 RC5 IDEA Blowfish	AEA DES* SKIPJACK	Contact NSA
Hash Algorithm	MD5 New standards as available	SHA 1 New standards as available	Contact NSA
Signature Algorithm	RSA EDSA	DSA	Contact NSA
Key Encryption Algorithm	RSA DH	KEA	Contact NSA
AEA - Advanced Encryption Algorithm DES- Digital Encryption Standard DH- Diffie-Hellman DSA - Digital Signature Algorithm EDSA - Elliptic Digital Signature Algorithm Hash- One way mathematical operation		IDEA - International Data Encryption Algorithm KEA - Key Encryption Algorithm MD5- Message Digest 5 RSA - Rivest-Shamir-Adleman SHA - Secure Hash Algorithm	

* - 3DES is currently recognized as a de facto standard, but has not been NIST Certified.

Table E3.5-4 Algorithm Robustness Examples

E3.6. Non-Technical Countermeasures. The defense in depth strategy relies on both technical and non-technical countermeasures as co-equal partners to establish and maintain an acceptable IA posture across the DoD. Non-technical countermeasures are discussed below.

E.3.6.1 Personnel Security: Personnel security is an integral part of the overall Information Assurance program. Specific requirements for personnel assigned to Information Assurance jobs can be found in DoD Regulation 5200.2R, "Personnel Security Program".

E.3.6.2 Physical Security: Physical Security is the action taken to protect DoD information technology resources (e.g. installations, personnel, equipment, electronic media, documents, etc.) from damage, loss, theft, or unauthorized physical access. Specific guidance can be found in DoD Regulation 5200.8, "Security of Military Installations and Resources."

E3.6.3 Procedural Security: Procedural Security is an integral part of the overall Information Assurance environment and supports the concepts of defense-in-depth. Procedural security measures both complement technical security measures, and can provide alternatives to technical security means when risk analysis indicates the use of procedures does not increase the overall risk to a system or network. Procedural Security provides the necessary actions, controls, processes, and plans to ensure continuous operation of a system or network within an accredited security posture, and is site and task dependent. Site security procedures shall be developed to supplement the security features of the hardware, software and firmware of information technology resources, to include such standardized processes as security training, user access control, media labeling and classified material handling.

E3.6.4. Security Training, Education and Certification. Security education, training, and awareness are essential to a successful IA program. Employees who are informed of applicable organizational policies and procedures can be expected to act effectively to ensure the security of system resources General users require different training than those employees with specialized responsibilities. Minimum IA training requirements to support D-i-D can be found in joint USD (P&R) and ASD (C3I) guidance (reference (p)).

E3.6.5. Marking and Labeling

E3.6.5.1. Storage Media: Information storage media will have external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. ISSO's and SA's shall identify the removable storage media to be used with a system. Classified removable media shall be controlled and protected in a manner similar to that used for classified paper materials.

E3.6.5.1.1. Removable media shall be marked as classified if the media has ever been used on the classified system, AND during any use on the system, was writeable (i.e., the write-protect feature could not be verified).

E3.6.5.1.2. Non-removable information storage media shall bear external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. If it is difficult to mark the non-removable media itself, the labels described below may be placed in a readily visible position on the cabinet enclosing the media.

E3.6.5.2 Marking Hardware Components. Procedures shall be implemented to ensure that all components of an IS, including input/output devices that retain information, terminals, standalone microprocessors, and word processors used as terminals, bear a conspicuous, external label. This label shall state the highest classification level and most restrictive classification category of the information accessible to the component in the IS. This labeling may consist of permanent markings on the component or a sign placed on the terminal.

E3.6.5.3. Marking Human-Readable Output.

E3.6.5.3.1. Human-readable output shall be marked appropriately, on each human-readable page, screen, or equivalent (e.g., the proper classification must appear on each classified microfiche *and* on each page of text on the fiche).

E3.6.5.3.2 Warning Banner: All individuals attempting access to DoD information systems shall be provided sufficient notice that use of official DoD information systems or networks constitutes consent to monitoring. Adequate warning shall be provided by clearly displaying the legally approved DoD warning banner. At a minimum, the DoD warning banner shall be displayed to the user upon initial entry/login to system, network, local, and remote resources. Acceptance of the banner warning screen shall constitute consent to monitoring.

E3.6.6. Standard Operating Procedures: Consistent, clearly documented operating procedures for both system configuration and operational use are key to ensuring information assurance. Procedures should define deployment of the system, system configuration, day to day operations for both the system administrator and user, as well as how to respond to real or perceived attempts to violate system security. All DoD information systems and networks shall include written standard operating procedures, which are routinely updated and tailored to reflect changes in the operational environment.

E3.6.7. Incident Reporting and Response: In addition to protective measures designed into information systems and architectures, sites should have a structured ability to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of DoD operations.

E3.6.7.1. Incident Reporting: All DoD organizations shall promptly report incidents via their appropriate chain of command. Types of incidents that will be reported include:

E3.6.7.1.1. Intrusion: Unauthorized access to an information system.

E3.6.7.1.2. Denial of Service Attacks: Actions which prevent any part of an automated information system from functioning in accordance with its intended purpose, to include any action which causes the unauthorized destruction, modification, or delay of service.

E3.6.7.1.3 Malicious Logic: Hardware, software, or firmware that is intentionally included in an information system for an unauthorized purpose, such as a virus or Trojan horse.

E3.6.7.1.4 Probe: In information operations, any attempt to gather information about an automated information system or its users online.

E3.6.7.2. Computer Incident Response: In accordance with the JTF-CND Concept of Operations dated December 1998, the JTF CND, serves as the DoD primary computer incident response capability to provide assistance in identifying, assessing, containing, and countering incidents that threaten DoD information systems and networks. The JTF CND will collaborate and coordinate DoD efforts with other Government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and information systems, and to minimize or eliminate identified vulnerabilities.

E3.6.7.3. COMSEC Material Incident Reporting: Incidents involving the compromise or the suspected compromise of COMSEC material or incidents that warrant further investigation shall be reported in accordance with NSTISSI 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, dated August 1997.

E3.6.8. Assessments

E3.6.8.1. Vulnerability Assessments: Vulnerability assessments identify vulnerabilities in an operational environment and validate a particular site's overall security posture and degree of system integration. Types of assessments include, but are not limited to:

E3.6.8.1.1. Monitoring: Monitoring is an on-line assessment to better understand the vulnerability of DoD systems.

E3.6.8.1.2 On-Line Surveys: On-line surveys conducted by Services and Defense agencies help DoD commands identify vulnerabilities on assigned and joint systems.

E3.6.8.2 Commands may request more detailed on-site assistance (e.g., on-site assessments and ISSE surveys) to better understand their vulnerabilities.

E3.6.8.3. Red Team Operations: Red Team operations may be employed to validate existing IA protections and to exercise standard operating procedures and tactics to evaluate vulnerabilities.

E3.6.9. Risk Management

E.3.6.9.1 Risk management is the discipline of identifying and measuring security risks associated with an information system, and controlling and reducing those risks to an acceptable level. The goal of risk management is to invest organizational resources to mitigate security risks in a cost-effective manner, while enabling timely and effective mission accomplishment. Risk management is an important aspect of information assurance and defense-in-depth.

E.3.6.9.2 The risk management process identifies assets to be protected, potential threats and vulnerabilities, and countermeasures and safeguards that can eliminate vulnerabilities or reduce them to levels acceptable for IS accreditation. Risk management is based on careful identification and evaluation of the threats and vulnerabilities that apply to a given IS and its operational environment.

E.3.6.9.3 Risk management is relevant to the entire life cycle of an IS. During IS development, security countermeasures are chosen. During IS implementation and operation, the effectiveness of in-place countermeasures is reconfirmed, and the effect of current threat conditions on system security is assessed to determine if additional countermeasures are needed to sustain the accredited IS's security. In scheduling risk management activities and designating resources, careful consideration should be given to Certification and Accreditation (C&A) goals and milestones. Associated risks can then be assessed and corrective action taken for unacceptable risks. Risk management requires the routine tracking and evaluation of the security state of an IS. The risk management process includes:

E.3.6.9.3.1 Analysis of the threats to and vulnerabilities of an information system, as well as of the potential impact that losing the system's information or capabilities would have on national security. This analysis forms a basis for identifying appropriate and cost-effective countermeasures.

E3.6.9.3.2 Risk mitigation. Analysis of trade-offs among alternative sets of possible safeguards.

E.3.6.9.3.3 Residual risk determination. Identification of the risk remaining after applying safeguards.

E.3.6.9.3.4 Acceptable level of risk. Judicious and carefully considered assessment by the appropriate DAA that the residual risk inherent in operating the IS after implementing all proposed security features is acceptable.

E.3.6.9.3.5 A reactive or responsive risk management process. To facilitate investigation of, and response to, incidents.

E.3.6.9.4 The risk management process applies both with all layers of the D-i-D strategy and the transition points between D-i-D layers. Interconnected systems pose risks that must be mitigated, in part, by further management processes

…..Risk accepted by one is risk imposed on all

E3.6.9.4.1. Configuration Management: Configuration management identifies, controls accounts for, and audits all changes made to a site or information system during its design, development, and operational lifecycle. Proper configuration management can substantially reduce and sometimes eliminate the need for costly complete re-accreditation. Appropriate levels of configuration management shall be established to maintain the accredited security posture. Each change or modification to an information system or site configuration shall assess the security impact of such a change against the security requirements and the accreditation conditions issued by the DAA.

E3.6.9.4.2. Data Management: The increasing reliance on distributed, interconnected information systems negates many of the data protection mechanisms built in to traditional "system high" networks and requires additional safeguards to protect DoD information from both unauthorized users and from authorized users without a need to know. Data processed, transmitted and stored on DoD information systems shall be protected to the appropriate level of classification or sensitivity and required level of IA.

E3.6.9.4.3 Requirements Management: For specific systems security requirements for passwords, marking guidance and implementation, account management, and operating systems security requirements, please refer to the Defense Information Infrastructure Common Operating Environment (DII COE) Software Requirements Specification for security version 4.0 dated 20 October 1998.

E3.6.10 System Security Policy: An Information System Security Policy (ISSP) shall be developed and maintained for every DoD organization employing information technology resources and for each information system used within the DoD. The ISSP shall identify the security requirements, objectives and policies implemented to safeguard

the site or system in a prescribed operational configuration, to include requirements for system redundancy and data backup and risk management decisions. Contingency plans will be developed and tested to prepare for emergency response, backup operations, and post-disaster recovery. This policy document will become part of the SSAA required by the DISTCAP (reference (j)).

INFORMATION ASSURANCE POLICY PANEL MEMBERSHIP

Donald. Jones	ASD(C3I)I&IA	(703) 614-6640	donald.l.jones@osd.pentagon.mil
Richard Hale	DISA D6A	(703) 681-2154	hale1r@ncr.disa.mil
Judy Bednar	ASD(C3I)I3	(703) 607-0253	bednarj@osd.pentagon.mil
Marti Pickens	ASD(C3I)DIAP	(703) 602-9981	pickensm@osd.pentagon.mil
Tom Green	ASD(HA)	(703) 681-3915	thomas.green@tma.osd.mil
CDR Chris Perry*	CNO/N6		
Lt Col Buzz Walsh**	JS/J6		
Capt Bill Wilson	AFCIC/SYNI	(703) 588-6148	william.f.wilson@pentagon.af.mil
Cliff Brown*	HQDA/ODISC4		
Howard Cohen	NSA/V21	(410) 854-7302	hhcohen@missi.ncsc.mil
Brian Henderson	NSA/I41	(410) 854-6831	bhenders@radium.ncsc.mil
Alan Riley	NSA/L1	(301) 688-3409	ariley@ncsc.mil
Joe Boyce	DIA/SYS-4	(202) 23108885	none
Monica Chandochin**	IC CIO		
Bruce Dubbs**	AF/CPSG		
Judy Munger	DFAS-HQ/SC	(703) 607-2070)	judy.munger@dfas.mil
Carol Letteer	DLA/C1	(703) 767-2198	carol_letteer@hq.dla.mil
John Hovath	DISA/D25	(703) 681-6486	horvathj@ncr.disa.mil
Deborah Robertson	MITRE	(703) 883-7155	nottingd@mitre.org
Bill Neugent	MITRE	(703) 883-6632	wneugent@mitre.org

* Since retired.
** Since reassigned